mIBS 方案的分析与改进 *

陈 明，冷建华

(宜春学院 数学与计算机科学学院，江西 宜春 336000)

摘 要：魏松杰等人提出一种基于安全仲裁 SEM(Security Mediator)的 mIBS(identity based signature)方案，利用 SEM 节点实现用户身份实时撤销。mIBS 方案中，SEM 持有部分用户私钥，与签名者共同完成签名。文章对 mIBS 方案进行了安全性分析，发现该方案存在严重安全缺陷，并给出一个具体的攻击实例。在攻击实例中，签名者通过与 SEM 的一次正常签名交互，窃取 SEM 持有的部分私钥，进而绕开 SEM 单独实施签名，使得 SEM 失效。文章提出一种改进的 mIBS 方案(记为 mIBSG)，对 SEM 持有的部分私钥增加了随机性保护。进一步，文章建立了 mIBS 方案安全模型 mEUF-CMIA(existential unforgeability under adaptive chosen message and identity attacks)，重点讨论了其敌手模型。除传统 IBS 敌手外，mEUF-CMIA 模型定义第 2 种类型敌手模拟一个恶意但合法的签名者，通过访问随机预言机，在没有 SEM 参与的情况下独立产生签名。在 mEUF-CMIA 模型下，mIBSG 方案的不可伪造性被规约为求解循环群上的 CDH 问题。对比分析表明，mIBSG 方案以较小的计算代价实现了可证明安全性。mIBSG 方案可用于构建基于 IBC 的跨域认证系统。

关键词：基于身份密码学；数字签名；计算 Diffie-Hellman 问题；随机预言机模型

中图分类号：TP309 doi: 10.19734/j.issn.1001-3695.2022.03.0130

Analysis and improvement of mIBS scheme

Chen Ming, Leng Jianhua

(*School of Mathematics & Computer Science*, *Yichun University*, *Yichun Jiangxi* 336000, *China*)

Abstract: Wei Songjie et al. proposed an identity-based signature scheme (named mIBS) , and used a security mediator (SEM) node to realize real-time revocation of entity identity in the mIBS scheme. The SEM held a part of the signature key, and generated a signature by working collaboratively with a signer. This paper analyzed the security of the mIBS scheme, found it had serious security flaws, and presented a specific attack instance. In the attack instance, a signer can stole the key held by the SEM through once normal signature interaction with a SEM, and then bypassed the SEM to implement a signature independently. This paper proposed an improved signature scheme (named mIBSG) . The mIBSG scheme remedied the security flaws of the original scheme by randomizing the private key held by the SEM. Further, this paper established a security model for mIBS scheme, named mEUF-CMIA, and defined a new type of adversary that simulated malicious but legitimate signers. The new adversary had the power to generate a forged signature independently through asking random oracles. Based on the new security model, this paper deduced the unforgeability of the mIBSG scheme as solving the CDH problem on a cyclic group. Comparative analysis showed that the mIBSG scheme achieved provable security with a small calculate efficiency loss. The mIBSG scheme can be used to build an IBC-based cross-domain authentication system.

Key words: identity based cryptography; digital signature; computational diffie-hellman problem; random oracle model

0 引言

基于身份密码学[1] (identity based cryptography, IBC)是由 Shamir 在 CRYPTO’84 会议上首次提出。IBC 系统将用户标识作为用户公钥，用户私钥由 KGC(key generation center)利用其主密钥生成并与用户标识关联。IBC 系统无须建立复杂的 PKI (public key infrastructure)，避免了公钥证书管理的沉重负担。直到 2001 年，Boneh 和 Franklin[2]基于双线性映射理论提出一种有效的 IBE(identity-based encryption)方案。随后，IBC 的研究成为一个热点。2007 年，RFC5091[3]草案将 Boneh-Franklin[2]算法推荐为基于身份加密标准，标志着 IBC 体制的标准化工作正式开启。2020 年，随着《信息安全技术 SM9 标识密码算法第 1 部分：总则》[4]、《信息安全技术 SM9 标识密码算法第 2 部分：算法》[5]获得批准，SM9 正式成为 IBC 算法国家标准，并逐步进入行业应用阶段。

然而，IBC 机制在拥有诸多优点的同时，也存在密钥托管、信任域网络规模较小等缺点。部分研究提出无证书[6,7]或自证书[8,9]等方案以解决 IBC 中的密钥托管问题；另一些研究则借鉴 PKI、区块链等技术和方法以扩大 IBC 域的网络覆盖范围[10~12]。区块链技术具有去中心化和数据不易被窜改等优点，利用区块链技术构建去中心化的信任域，可以确保跨域认证模型内第三方服务器的可信性。近来，多位研究者提出基于区块链技术的跨域认证模型和方案。马晓婷等人[11]基于国密 SM9，采用区块链技术构建了 PKI 与 IBC 联盟链模型，及其该模型下的跨域认证方案；黄穗等人[13]也提出了基于区块链的跨域认证模型，通过智能合约在区块链上构造布谷鸟过滤器，解决大规模证书查询请求的性能问题；魏欣等人[14]结合区块链与边缘计算思想，构建了一种适用于物联网的跨域认证架构，通过引入边缘网关屏蔽物联网的底层异构性，增强节点隐私保护；张亚兵等人[15]提出多层区块链的跨域认证方案，引入委托权益证明来评估节点的可信度，解决跨域访问时存在的多个管理域相互信任问题；魏松杰等人[12]提出

收稿日期：2022-03-09；**修回日期：**2022-05-12 **基金项目：**国家自然科学基金资助项目(61662083)

作者简介：陈明(1978-)，男，重庆北碚人，副教授，博士，主要研究方向为密码学、安全协议、教育技术（chenming9824@aliyun.com)；冷建华(1978-)，男，江西上高人，副教授，硕士，主要研究方向为信息安全、教育技术.

一种基于 IBC 和区块链的跨域认证协议，定义了基于仲裁的 IBC 域结构，并提出基于仲裁的身份签名 mIBS 和认证方案。在基本 IBC 系统基础上，mIBS 方案中引入安全仲裁 SEM (Security Mediator)具体实施对用户标识和密钥的撤销与核验。但是，魏松杰等人[12]对 mIBS 方案的安全性分析比较简单，没有定义合理的安全模型，存在严重的安全缺陷。

本文的主要工作包括三个方面：a)对魏松杰等人[12]提出的 mIBS 方案进行了全面的安全性分析。与传统的基于身份签名方案不同，mIBS 方案存在两类敌手，除传统敌手外，一个恶意的签名者也能对算法形成攻击。本文给出了一个针对 mIBS 方案的攻击实例，签名者通过与 SEM 的一次正常交互，获取了 SEM 持有的部分私钥，进而可以绕开 SEM，实施独立的签名认证。b)提出了改进的 mIBS 方案，记为 $\mathrm{mIBS_G}$ 方案，改进方案主要针对 mIBS 方案的缺陷进行了算法增强。c) 以 EUF-CMIA (existential unforgeability under adaptive chosen message and identity attacks)模型[16]为基础，定义了 mIBS 方案的安全模型，对两类敌手的行为进行了形式化定义。然后，采用新的模型对 $\mathrm{mIBS_G}$ 方案进行了安全规约，将 $\mathrm{mIBS_G}$ 方案的安全性规约为求解定义在循环群上的 CDH(computational Diffie-Hellman)问题。对比分析表明，改进方案以较小的计算代价实现了方案的可证明安全性。

1　背景知识

本节简要介绍相关的数学背景知识，详细内容可以参考文献[17]。

双线性映射：给定安全参数λ，初始化产生阶为大素数 p ($p>2^{\lambda}$)的循环群(G_1,+)和(G_2,×)，令 P 为 G_1 的生成元，如果给定的映射 $e: G_1\times G_1\rightarrow G_2$ 满足下列性质，则 e 是从 G_1 到 G_2 的一个双线性映射。

a) 双线性：给定 $U,V\in G_1$ 和任意的 $a,b\in\mathbb{Z}_p^*$，有 $e(U^a,V^b)=e(U,V)^{ab}$。

b) 非退化性：$e(P,P)\neq 1$。

c) 可计算性：给定 $U,V\in G_1$，能有效计算 $e(U,V)$。

CDH 问题：对于任意未知的 $a,b\in\mathbb{Z}_p^*$，给定 $P,aP,bP\in G_1$，求解 abP。

CDH 假设：如果不存在多项式时间算法在时间 t 内以至少 ϵ 的概率求解 CDH 问题，那么称(ϵ, t)- CDH 假设在 G_1 上成立。

本文研究的算法以 CDH 假设为基础。

2　mIBS 方案分析

本节首先简要回顾文献[12]提出的 mIBS 方案，然后对其安全性进行分析，提出有效的攻击实例。

2.1　mIBS 方案介绍

文献[12]提出一种基于 IBC 和区块链的跨域认证协议，并且提出一种 mIBS 方案用于在跨域认证中对信息服务实体 ISE 进行认证。为了解决基于身份密码系统中对实体身份的撤销等有效管理，在 mIBS 方案中引入安全仲裁(Security Mediator, SEM)，其系统框架如图 1。

在图 1 所示的 IBC 系统中，密钥生成中心 KGC 为用户生成两部分的私钥，其中一部分发回给用户，而另一部分私钥发送给 SEM。当用户需要进行签名的时候，首先向 SEM 申请签名信令，然后根据 SEM 返回的签名信令生成完整的签名。具体步骤简单描述如下。

Setup：给定系统参数(λ, p, P, G_1, G_2, e)如第 1 节所述，然后选择密码哈希函数 $H_1:\{0,1\}^*\rightarrow G_1^*$ 和 $H_2:\{0,1\}^*\times G_2^*\rightarrow\mathbb{Z}_p^*$，其中，$G_1^*$ 和 G_2^* 分别表示 $G_1/\{0\}$ 和 $G_2/\{1\}$。KGC 随机选择 $s\in[1,p-1]$ 作为系统主密钥，计算 $P_{\mathrm{pub}}=[s]P\in G_1$ 作为系统主公钥，其中，$[s]$ 表示取整运算。KGC 秘密保存系统主密钥 s，并公开系统参数 pp=(λ, p, P, G_1, G_2, e, P_{pub}, H_1, H_2)。

KeyGen：用户提交身份标识 $ID\in\{0,1\}^*$，KGC 首先计算 $P_{ID}=H_1(ID)\in G_1^*$，$d_{ID}=[s]P_{ID}\in G_1^*$，然后随机选择 $s_{ID}\in[1,p-1]$ 并计算 $d_{ID}^{\mathrm{user}}=[s_{ID}]P_{ID}, d_{ID}^{\mathrm{SEM}}=d_{ID}-d_{ID}^{\mathrm{user}}=[s-s_{ID}]P_{ID}$。KGC 将 d_{ID}^{user} 通过安全信道发送给用户，将 d_{ID}^{SEM} 通过安全信道发送给 SEM。

Sign：按如下步骤计算消息签名。

a) 给定消息 $m\in\{0,1\}^*$，用户随机选择 $P_1\in G_1$ 和 $k\in\mathbb{Z}_p^*$，计算 $q=e(kP_1,P)$，$g=H_2(m,q)$ 和 $S_{\mathrm{user}}=kP_1+gd_{ID}^{\mathrm{user}}$，向 SEM 发送签名信令请求($ID$, q, g, S_{user})。

b) SEM 收到(ID, q, g, S_{user})后，首先检索用户 ID，若该身份已被撤销则停止，否则计算 $S_{\mathrm{SEM}}=gd_{ID}^{\mathrm{SEM}}$ 和 $S_m=S_{\mathrm{user}}+S_{\mathrm{SEM}}$，然后计算 $P_{ID}=H_1(ID)$ 和 $q'=e(S_m,P)\cdot e(P_{ID},-P_{\mathrm{pub}})^g$；判断 $q'=q$ 是否成立，若成立则发送 S_{SEM} 给用户。

c) 用户收到 S_{SEM} 后，按 b)的方式计算 S_m 和 q'，若 $q'=q$ 成立则输出签名(ID, m, g, S_m)，否则重新申请签名信令。

Verify：对签名(ID, m, g, S_m)的验证。首先按照 Sign 算法中 b)的方式计算 q'，然后计算 $g'=H_2(m,q')$，如果 $g'=g$ 成立，则接受签名。

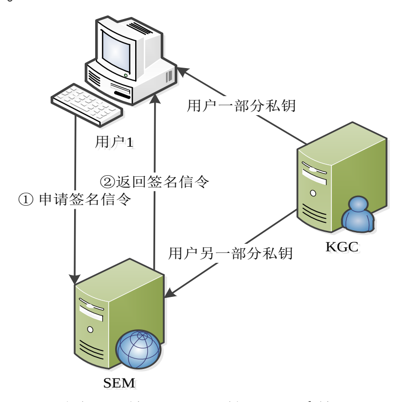


图 1　基于 SEM 的 IBC 系统

Fig. 1　SEM-based IBC system

2.2　mIBS 方案安全性分析

文献[12]对 mIBS 方案进行了简单的安全性分析，没有建立完整的安全模型。由于 mIBS 方案中引入 SEM 实体，并且将用户的私钥分成了两个部分，因此，针对 IBS 方案的 EUF-CMIA 模型[16]在本方案中不完全适用。本节将提出一种针对 mIBS 方案的新攻击方法。

首先，原方案中存在一定的计算错误概率。具体来说，在签名验证计算式 $gd_{ID}^{\mathrm{user}}+gd_{ID}^{\mathrm{SEM}}=g([s_{ID}]+[s-s_{ID}])P_{ID}$ 中，等式 $([s_{ID}]+[s-s_{ID}])=[s]$ 并不一定成立。这会使得用户的私钥无效。

由于真实密码算法的密钥非常大，这里以小的模数 $p=23$ 来举例说明，即：$s,s_{ID}\in[1,22]$。

根据 Setup 算法和 KeyGen 算法，假设 KGC 随机选择 s=10.3，s_{ID}=5.7，以上下取整为例，则 $[s]$=[10.3]=10，$[s_{ID}]$=[5.7]=6，$[s\text{-}s_{ID}]$= [10.3-5.7]=[4.6]=5，那么：($[s_{ID}]$+$[s-s_{ID}]$) =11≠$[s]$。如果采用上取整或下取整也存在类似情况。简单估算，上述错误概率接近 1/2。一种改进方法是：在 KeyGen 算法中，对 $([s_{ID}]+[s-s_{ID}])=[s]$ 进行验算，如果等式成立则输出私钥，如果不成立，则重新选择私钥，使得等式成立。更一般的解决方案是：主密钥 s 和用户秘密 s_{ID} 从 $\mathbb{Z}_p^*$ 中随机选择。

另外，文献[12]将对 $S_{\mathrm{SEM}}=g(s-s_{ID})P_{ID}$ 的攻击规约为求解离散对数问题，即，求解 $(s-s_{ID})$。这一规约路径是错误的，因为 SEM 持有的部分私钥是 $(s-s_{ID})P_{ID}\in G_1^*$，而不是 $(s-s_{ID})$。因此，攻击者只需要获得 $(s-s_{ID})P_{ID}$ 就可以伪造任何的签名信令 $S'_{\mathrm{SEM}}=g'(s-s_{ID})P_{ID}$，使得 $g'\neq g$ 且 $S'_{\mathrm{SEM}}\neq S_{\mathrm{SEM}}$。进而，签名者可以绕开 SEM，实施独立的签名，使得 SEM 无效，具体签名过程简单描述如下。这里忽略上述计算错误，即假定用户的

私钥是有效的，满足：等式 $([s_{ID}]+[s-s_{ID}])=[s]$ 成立的条件。

a) 签名者从 SEM 收到一个有效的 $S_{\mathrm{SEM}}=g(s-s_{ID})P_{ID}$ 后，首先求 g 关于 $\bmod p$ 的乘法逆元 $g^{-1}\in\mathbb{Z}_p^*$，即，$g^{-1}g\equiv 1 \bmod p$。由于 p 为素数，因此一定存在 $g^{-1}\in\mathbb{Z}_p^*$，且多项式时间可计算。然后，计算 $d_{ID}^{\mathrm{SEM}}=g^{-1}S_{\mathrm{SEM}}=g^{-1}g(s-s_{ID})P_{ID}=(s-s_{ID})P_{ID}$。注意，为了描述简洁，在非必要的场景下，文中关于循环群上的运算表达式省略了 $\bmod p$ 运算。

b) 给定消息 $m'\in\{0,1\}^*$，签名者随机选择 $P_1'\in G_1$ 和 $k'\in\mathbb{Z}_p^*$，计算 $q'=e(k'P_1',P)$，$g'=H_2(m',q')$ 和 $S_{\mathrm{user}}'=k'P_1'+g'd_{ID}^{\mathrm{user}}$，然后计算 $S_{\mathrm{SEM}}'=g'd_{ID}^{\mathrm{SEM}}$ 和 $S_m'=S_{\mathrm{user}}'+S_{\mathrm{SEM}}'$，输出签名 (ID,q',g',S_m')。

可以验证：

$$\begin{aligned}&e(S_m',P)\cdot e(P_{ID},-P_{\mathrm{pub}})^{g'}=\\&e(k'P_1'+g'd_{ID}^{\mathrm{user}}+g'd_{ID}^{\mathrm{SEM}},P)\cdot e(P_{ID},-P_{\mathrm{pub}})^{g'}=\\&e(k'P_1',P)\cdot e([s]P_{ID},P)^{g'}\cdot e(P_{ID},[s]P)^{-g'}=e(k'P_1',P)=q'\end{aligned}\tag{1}$$

可见，由于签名者获得了 SEM 持有的部分私钥，可以独立实施对任意消息的签名，攻击成立。

3 改进的 mIBS 方案及其安全性分析

本章首先对原有 mIBS 方案的改进方案，记为 mIBS$_G$，然后讨论其安全模型，并对改进方案进行安全性分析。

3.1 mIBS 方案改进

考虑 2.2 节中对 mIBS 方案的伪造攻击。攻击形成的关键原因是在 SEM 签署的签名信令 $S_{\mathrm{SEM}}=gd_{ID}^{\mathrm{SEM}}$ 中缺少对部分私钥 d_{ID}^{SEM} 的随机性保护，导致恶意的签名者通过一次确定的签名过程直接恢复出 SEM 持有的部分私钥 d_{ID}^{SEM}。因此，本文的改进方案则在原方案的基础上，在 Sign 算法中添加对 d_{ID}^{SEM} 的随机性保护，具体描述如下。

mIBS$_G$ 方案不改变原有方案的总体框架，系统建立(Setup)和密钥生成(KeyGen)与原方案基本相同。在系统公开参数中增加密码哈希函数 $H_3:\mathbb{Z}_p^*\times G_2^*\to\mathbb{Z}_p^*$；密钥生成阶段要求 KGC 检验等式 $([s_{ID}]+[s-s_{ID}])=[s]$ 是否成立，如果不成立则重新生成密钥，直到等式成立。签名和签名签证过程如下所述。

Sign：按如下步骤计算消息签名。

a) 给定消息 $m\in\{0,1\}^*$，用户随机选择 $P_1\in G_1$ 和 $k\in\mathbb{Z}_p^*$，计算 $q_1=e(kP_1,P)$，$g=H_2(m,q_1)$ 和 $S_{\mathrm{user}}=kP_1+gd_{ID}^{\mathrm{user}}$，向 SEM 发送签名信令请求$(ID, q_1, g, S_{\mathrm{user}})$。

b) SEM 收到$(ID, q_1, g, S_{\mathrm{user}})$后，首先检索用户 ID，若该身份已被撤销则停止，否则随机选择 $P_2\in G_1$，计算 $q_2=e(P_2,P)$，$r=H_3(g,q_2)$，$S_{\mathrm{SEM}}=r(P_2+gd_{ID}^{\mathrm{SEM}})$ 和 $S_m=rS_{\mathrm{user}}+S_{\mathrm{SEM}}$，然后计算 P_{ID}=$H_1(ID)$，并验证等式 $(q_1\cdot q_2)^r=e(S_m,P)\cdot e(P_{ID},P_{\mathrm{pub}})^{-rg}$ 是否成立，若成立则发送 (q_2,S_{SEM}) 给用户。

c) 用户收到 (q_2,S_{SEM}) 后，计算 $r=H_3(g,q_2)$，以及完整签名 $S_m=rS_{\mathrm{user}}+S_{\mathrm{SEM}}$，验证等式 $(q_1\cdot q_2)^r=e(S_m,P)\cdot e(P_{ID},P_{\mathrm{pub}})^{-rg}$ 是否成立，若成立则输出签名(ID, m, q_1, q_2, S_m)，否则重新申请签名信令。

Verify：对签名(ID, m, q_1, q_2, S_m)的验证。签名验证者首先计算 $g=H_2(m,q_1)$，$r=H_3(g,q_2)$ 和 P_{ID}=$H_1(ID)$，然后验证等式 $(q_1\cdot q_2)^r=e(S_m,P)\cdot e(P_{ID},P_{\mathrm{pub}})^{-rg}$ 是否成立，若成立则接受签名。

可以验证：

$$\begin{aligned}&e(S_m,P)\cdot e(P_{ID},P_{\mathrm{pub}})^{-rg}=\\&e(rkP_1+rgd_{ID}^{\mathrm{user}}+rP_2+rgd_{ID}^{\mathrm{SEM}},P)\cdot e(P_{ID},P_{\mathrm{pub}})^{-rg}=\\&e(rkP_1,P)\cdot e(rP_2,P)\cdot e(d_{ID}^{\mathrm{user}}+d_{ID}^{\mathrm{SEM}},P)^{rg}\cdot e(P_{ID},P_{\mathrm{pub}})^{-rg}=\\&e(kP_1,P)^r\cdot e(P_2,P)^r\cdot e([s]P_{ID},P)^{rg}\cdot e(P_{ID},[s]P)^{-rg}=\\&(q_1\cdot q_2)^r\end{aligned}\tag{2}$$

由式(2)可得，mIBS$_G$ 方案具有可验证正确性。

在 mIBS$_G$ 方案中，在 Sign 算法的 b)步骤，本文增加了随机选择的 $P_2\in G_1$，并且利用 $r=H_3(g,q_2)$ 将 g 与 $q_2=e(P_2,P)$ 进行了绑定。由于 P_2 是随机的，因此从任何敌手的视角来看，$q_2=e(P_2,P)$ 也是随机的。本质上，签名信令 (q_2,S_{SEM}) 是 SEM 采用部分私钥 d_{ID}^{SEM} 对签名请求消息 $g=H_2(m,q_1)$ 的签名，主要目的是防止签名者任意替换消息 g，确保了签名者每次签名都必须请求 SEM 产生一个新的签名信令。同时，由于存在新鲜且随机的 $P_2\in G_1$，任何敌手想要从 $S_{\mathrm{SEM}}=r(P_2+gd_{ID}^{\mathrm{SEM}})$ 中恢复出部分私钥 d_{ID}^{SEM}，都面临求解 CDH 问题。详细的安全性分析，请见本文 3.2 节。

3.2 mIBSG 方案安全性分析

本节首先建立 mIBS 方案安全模型，然后对 mIBS$_G$ 方案进行安全性规约。

3.2.1 mIBS 安全模型

下面首先回顾基本的 EUF-CMIA 模型[16]。

定义敌手 A 与模拟器 B 之间的 EUF-CMIA 游戏如下。

系统建立：B 执行 Setup 算法，公开系统公共参数 pp，创建 N 个用户的身份集合 $\partial_{\mathrm{ID}}=\{ID_1,\ldots,ID_N\}$，并且随机选择用于挑战的用户身份 $ID^*\in\partial_{\mathrm{ID}}$。

询问：A 自适应地执行多项式时间有界次的询问。

KeyGen 询问。A 提交用户身份 ID，B 返回其私钥 sk_{ID}。这里要求 A 不能询问 ID^* 的私钥。

Sign 询问。A 提交(ID, m)，B 返回签名 σ 给 A。

伪造：询问阶段结束以后，A 输出伪造签名(ID^*, m^*, σ^*)。

定义 1 对 IBS 方案 $\Im=(\mathrm{Setup},\mathrm{KeyGen},\mathrm{Sign},\mathrm{Verify})$，敌手 A 在选择身份攻击下的优势定义为

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{EUF-CMIA}}=\Pr\left[\begin{array}{l}\mathrm{pp}\leftarrow\mathrm{Setup}(1^{\lambda})\\(ID,sk)\leftarrow\mathrm{KeyGen}(\mathrm{pp},ID)\\(m^*,\sigma^*)\leftarrow\mathcal{A}^{\mathrm{O_{Sign}}(\cdot)}(\mathrm{pp})\end{array}:\begin{array}{c}m^*\notin\partial_{\mathrm{m}}\wedge\\ Verify(ID^*,m^*,\sigma^*)=1\end{array}\right]$$

其中，$\mathrm{O_{Sign}}(\cdot)$ 是一个签名预言机，模拟 Sign 询问，集合 ∂_{m} 存储已完成签名询问的消息 m 及其对应的签名应答 σ。如果对于任意多项式时间敌手 A，有 $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{EUF-CMIA}}=\mathrm{negl}(\lambda)$ 成立，则称 $\Im$ 在选择身份攻击下具有不可伪造性。

引理 1 令 $\Im$ 是一种数字签名机制，其安全参数为λ。A 是一个概率多项式时间图灵机，其输入为公开参数。A 可以自适应地完成随机预言机(random oracle, RO)询问，假设 A 以概率 $\epsilon(\lambda)$ 输出一个有效的签名 $\sigma^*=(ID^*,m^*,q_1^*,q_2^*,r^*,g^*,S_m^*)$，则存在一个算法 $\mathcal{A}'$ 利用 A，在多项式时间内产生两个有效的签名 $\sigma^*=(ID^*,m^*,q_1^*,q_2^*,r^*,g^*,S_m^*)$ 和 $\sigma'=(ID^*,m^*,q_1^*,q_2^*,r',g',S_m')$，使得 $r^*\neq r'\wedge g^*\neq g'$ 成立。

引理 1 是数字签名安全性证明中广泛采用的分叉引理[18](forking lemma)，由 Pointcheva 等人首次引入。本文安全模型也引用这一引理。

根据 2.2 节的分析，mIBS 方案与基本 IBS 方案存在较大差异，同时存在两类敌手。第 1 类是传统的 IBS 敌手，其攻击目标是伪造完整的签名；第 2 类敌手是恶意的签名者，其攻击目标是伪造签名信令。因此，对 mIBS 方案的分析模型应对基本的 EUF-CMIA 模型进行调整，本文定义为 mEUF-CMIA 模型。

mEUF-CMIA 模型的主要变化在于刻画敌手的能力。对于第 1 类敌手，限制其询问 ID^* 的完整私钥；对于第 2 类敌手，允许其询问 ID^* 的部分私钥($d_{ID^*}^{\mathrm{user}}$)，而不允许其询问 ID^* 的另一部分私钥($d_{ID^*}^{\mathrm{SEM}}$)。此外，针对两类敌手提交的 Sign 询问，模拟器 B 应答的方式也有所区别。具体内容见 3.2.2 节。

3.2.2 mIBSG 方案安全性证明

本节对 mIBS$_G$ 方案进行安全性规约，基于 CDH 假设，证明其在选择身份和选择消息攻击下具有不可伪造性。

首先对规约过程进行简单的非形式化分析。给定 CDH 实例 (P,aP,bP)，令 KGC 的主公钥为 aP，令 $H_1(ID^*)=bP$（ID^* 为挑战用户身份），则 ID^* 的私钥为 $d_{ID}=d_{ID}^{\mathrm{user}}+d_{ID}^{\mathrm{SEM}}=[s]P_{ID}=abP$。在 mEUF-CMIA 游戏中，KGC 的主密钥 $[s]=a$ 是未知的，因此

ID^* 的完整私钥 d_{ID} 包含了一个 CDH 问题的实例。通过游戏模拟，模拟器 B 利用 A 输出 ID^* 签名来求解该 CDH 问题实例。如果 CDH 假设成立，那么 B 成功的优势是可以忽略的，从而反证 A 成功伪造 ID^* 签名的优势也是可以忽略的。

在基于随机预言机的安全模型中，哈希函数通常被替换为哈希询问，称为哈希预言机(Hash Oracle)。

定理 1　如果 CDH 假设成立，那么本文 mIBS$_G$ 方案满足 EUF-CMIA 安全。

证明　假设存在多项式时间敌手 A 以不可忽略的优势攻破 mIBS$_G$ 方案，本文将构建一个算法 B 利用 A，在多项式时间内解决 CDH 问题。给定 CDH 实例 (P, aP, bP)，下面模拟 B 与 A 的 mSID-EUF-CMA 游戏。

系统建立：B 运行 Setup 算法，产生系统公开参数 pp=(λ, $p, P, G_1, G_2, e, P_{pub}$)，创建 N 个用户的身份集合 $\partial_{ID}=\{ID_1,\ldots,ID_N\}$，并将 pp 和 ∂_{ID} 发送给 A。其中，$P_{pub}=aP$，即系统主密钥 $s=a$ 未知。B 随机选择用于挑战的用户身份 $ID^*\in\partial_{ID}$。注意，根据随机预言机假设，模拟过程中，用哈希询问(H$_1$, H$_2$, H$_3$)替换哈希函数(H_1, H_2, H_3)。

询问：A 自适应地执行多项式时间有界次的询问。B 维护初始为空的列表(L$_1$, L$_2$, L$_3$, L$_k$, ∂_m)。

H$_1$ 询问。A 提交 $H_1(ID_i)$ 询问。如果 ID_i 在列表 L$_1$ 中存在，则直接返回 P_i；否则，如果 $ID_i\in\partial_{ID}\wedge ID_i\neq ID^*$，B 随机选择 $t_i\in\mathbb{Z}_p^*$，计算 $P_i=t_iP$，将 (ID_i,t_i,P_i) 插入集合 L$_1$；如果 ID_i=ID^*，则令 $P_i=bP$，将 $(ID^*,\perp,P_i)$ 插入集合 L$_1$。最后将 P_i 返回给 A。

H$_2$ 询问。A 提交 $H_2(m_i,q_{1,i})$ 询问。如果 $(m_i,q_{1,i})$ 在列表 L$_2$ 中存在，则 B 直接返回对应的 g_i；否则，B 随机选择 $g_i\in\mathbb{Z}_p^*$，并返回给 A，然后将 $(m_i,q_{1,i},g_i)$ 插入 L$_2$。

H$_3$ 询问。A 提交 $H_3(g_i,q_{2,i})$ 询问。如果 g_i 在列表 L$_2$ 中不存在，则返回⊥；否则，如果 $(g_i,q_{2,i})$ 在列表 L$_3$ 中存在，则 B 直接返回对应的 r_i；否则，B 随机选择 $r_i\in\mathbb{Z}_p^*$，并返回给 A，然后将 $(g_i,q_{2,i},r_i)$ 插入 L$_3$。

KeyGen 询问。A 提交身份 ID_i。

a) 如果 $ID_i\in\partial_{ID}\wedge ID_i\neq ID^*$，且 $(ID_i,d_i^{user},d_i^{SEM})$ 在 L$_k$ 中存在，B 直接返回 (d_i^{user},d_i^{SEM}) 给 A；否则，B 通过 H$_1$ 询问得到 (ID_i,t_i,P_i)，随机选择 $s_i\in[1,p-1]$，计算 $d_i^{user}=[s_i]P_i$，$d_i^{SEM}=t_iP_{pub}-[s_i]P_i$，将 (d_i^{user},d_i^{SEM}) 返回给 A，并将 $(ID_i,d_i^{user},d_i^{SEM})$ 插入 L$_k$。可以验证：$d_i^{SEM}=t_iP_{pub}-[s_i]P_i=\ (a-[s_i])P_i$。因此，从敌手的视角来看，KeyGen 询问输出与真实密钥生成算法输出的密钥同分布且不可区分。

b) 如果 ID_i=ID^*，B 随机选择 $s_i\in[1,p-1]$，令 $P_i=bP$，计算 $d_i^{user}=[s_i]P_i$，将 $(ID_i,d_i^{user},\perp)$ 插入 L$_k$。如果 A 是第 1 类敌手，则返回⊥；如果 A 是第 2 类敌手，则返回 d_i^{user} 给 A。

Sign 询问。A 提交 $\mathrm{Sign}(ID_i,m_j)$ 询问。如果 ID_i 的私钥还未创建，则 B 首先按照 KeyGen 询问的方法创建用户私钥。如果 $ID_i\in\partial_{ID}\wedge ID_i\neq ID^*$，B 按照 mIBS$_G$ 方案的 Sign 算法计算并输出签名 $\sigma_j=(ID_i,m_j,q_{1,j},q_{2,j},S_{m_j})$，然后将 σ_j 插入 ∂_m。如果 ID_i=ID^*，为了区分两类敌手，本文分别构建两种形式的 Sign 应答。

a) 如果 A 是第 1 类敌手。B 随机选择 $P_{1,j}\in G_1$ 和 $k_j\in\mathbb{Z}_p^*$，计算 $q_{1,j}=e(k_jP_{1,j},P)$，通过 $H_2(m_j,q_{1,j})$ 询问获得 g_j，然后计算 $S_{user,j}=k_jP_{1,j}+g_jd_i^{user}$，接着随机选择 $r_j\in\mathbb{Z}_p^*$ 和 $S_{SEM,j}\in G_1$，计算 $S_{m,j}=r_jS_{user,j}+S_{SEM,j}$，令 $q_{2,j}=e(S_{m,j},P)^{r_j^{-1}}\cdot e(P_i,P_{pub})^{-g_j}\cdot q_{1,j}^{-1}$，然后将 $(g_i,q_{2,i},r_i)$ 插入 L$_3$。最后，B 将 $\sigma_j=(ID_i,m_j,q_{1,j},q_{2,j},S_{m_j})$ 插入 ∂_m，并且返回签名 σ_j 给 A。

b) 如果 A 是第 2 类敌手。A 提交签名信令请求 $(ID_i,q_{1,j},g_j,S_{user,j})$。如果 $(q_{1,j},g_j)$ 在列表 L$_2$ 中不存在或不匹配，则 B 返回⊥；否则，B 随机选择 $r_j\in\mathbb{Z}_p^*$ 和 $S_{SEM,j}\in G_1$，计算 $S_{m,j}=r_jS_{user,j}+S_{SEM,j}$，令 $q_{2,j}=e(S_{m,j},P)^{r_j^{-1}}\cdot e(P_i,P_{pub})^{-g_j}\cdot q_{1,j}^{-1}$，然后将 $(g_i,q_{2,i},r_i)$ 插入 L$_3$。最后，B 将 $\sigma_j=(ID_i,m_j,q_{1,j},q_{2,j},S_{m_j})$ 插入 ∂_m，并且返回签名 σ_j 给 A。

容易验证，等式：$(q_1\cdot q_2)^r=e(S_m,P)\cdot e(P_i,P_{pub})^{-rg}$ 成立。在真实签名算法中，$q_{2,j}=e(P_{2,j},P)$。其中，$P_{2,j}\in G_1$ 由 SEM 随机选择，且独立于(两类)敌手的视角，进而 $q_{2,j}$ 也独立于敌手的视角。也就是说，从敌手的视角来看，Sign 询问的输出与真实签名算法的输出同分布且不可区分。

伪造：询问阶段结束以后，A 输出伪造签名 $\sigma^*=(ID,m^*,q_1^*,q_2^*,S_m^*)$。

如果 $ID\neq ID^*\vee m^*\in\partial_m$，B 终止游戏，模拟失败。否则，B 以 (q_1^*,q_2^*) 为索引查询列表 L$_2$/L$_3$ 取得 (r^*,g^*)，若验证等式：$(q_1^*\cdot q_2^*)^{r^*}=e(S_m^*,P)\cdot e(P_{ID^*},P_{pub})^{-r^*g^*}$ 成立，则 A 赢得游戏。如果 (r^*,g^*) 在 L$_2$/L$_3$ 中不存在，则终止游戏，模拟失败。也就是说，A 必须通过哈希询问取得 (r^*,g^*)，这就保证了计算顺序 $q_1^*\to g^*,q_2^*\to r^*$，从而使得敌手无法采用 Sign 询问中的方法构造伪造签名。在真实世界中，哈希预言机是不存在的，因此，Sign 询问中的签名构造方法是无法实现的，这是随机预言机模型与真实世界的主要区别。

如果游戏没有终止，且 A 赢得游戏。根据分叉引理[18]，B 可以构造算法 $\mathcal{A}'$ 利用 A 产生另一有效签名 $(ID^*,m^*,q_1^*,q_2^*,r',g',S_m')$，$r^*\neq r'\wedge g^*\neq g'$。可以验证：

$$S_m^*=r^*k^*P_1^*+r^*P_2^*+r^*g^*(d_{ID^*}^{user}+d_{ID^*}^{SEM})=r^*(k^*P_1^*+P_2^*)+r^*g^*(abP) \tag{3}$$

$$S_m'=r'k^*P_1^*+r'P_2^*+r'g'(d_{ID^*}^{user}+d_{ID^*}^{SEM})=r'(k^*P_1^*+P_2^*)+r'g'(abP) \tag{4}$$

根据式(3)(4)，B 计算：

$$abP=(g'-g^*)^{-1}(r'^{-1}S_m'-r^{*-1}S_m^*) \tag{5}$$

作为对 CDH 问题的回答。

令 A 赢得游戏的优势为 $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{mSID-EUF-CMA}}=\epsilon$，那么 B 赢得 CDH 挑战的优势为：$\epsilon'=\epsilon+\mathrm{negl}(\lambda)$。

根据 CDH 假设，如果 B 赢得 CDH 挑战的优势 ϵ' 是可忽略的，那么 A 赢得游戏的优势也是可忽略。

证毕。

4　对比分析

在安全性方面，本文 mIBS$_G$ 方案实现了在随机预言机模型下的可证明安全。mIBS 方案[12]则存在安全缺陷，签名者可以绕开 SEM 独立实施签名，违背了 mIBS 方案的设计初衷。

计算开销方面，mIBS$_G$ 方案与原方案的对比如表 1 所示。表中列举了主要的计算开销，其中，P 表示双线性对运算，H 表示哈希运算，M 表示群 G_1/G_2 上的乘法运算，A 表示群 G_1/G_2 上的加法运算，E 表示群 G_2 上的指数运算。在群 G_1 上和群 G_2 上的乘法(加法)运算时间差别不大，因此合并计算。

表 1　计算开销对比

Tab. 1　Comparison of computational costs

Algorithms	Sign		Verify
	Signer	SEM	Signature Verifier
mIBS	3P+3M+2A+1E+1H2	2P+2M+1A+1E+1H1	2P+1M+1E+1H1+1H2
mIBSG	3P+5M+2A+2E+1H2+1H3	3P+4M+2A+2E+1H1+1H2	2P+2M+2E+1H1+1H2+1H3

从各类计算开销来看，签名者增加(2M+1E+1H$_3$)，SEM 增加(1P+2M+1A+1E+1H$_2$)，验证者则增加(1M+1E+1H$_3$)。根据文献[12]给出的实验环境和实验数据：1 次双线性对运算时间约等于 1.112ms，1 次 G_1/G_2 上的乘法运算时间约等于 0.407ms，1 次 G_1/G_2 上的加法运算时间约等于 0.003ms，1 次 G_2 上的指数运算时间约等于 0.131ms。而哈希函数的计算时

间相较来说则更低，可以忽略不计。因此，从时间开销上来说，增加较多的是 SEM，总的计算时间约为 5.232ms，增加约 2.06ms。

5 结束语

魏松杰等人[12]提出一种 mIBS 方案，引入安全仲裁 SEM 对 IBC 域中用户身份进行撤销管理和核验。但是，分析发现，该方案存在严重安全缺陷，签名者可利用与 SEM 的一次正常交互，获取 SEM 持有的部分私钥。本文提出改进的 $mIBS_G$ 方案，并建立了安全模型。新安全模型在传统 SID-EUF-CMA 模型的基础上定义了两类敌手，分别模拟外部攻击者和恶意的签名者。在新的安全模型下，$mIBS_G$ 方案的不可伪造性被规约为求解循环群上的 CDH 问题，实现了可证明安全性。

总体来看，mIBS 算法效率不具有比较优势，后续优化研究可以从以下两方面展开。第一，实际应用中，网络延迟所消耗的时间远远大于节点计算时间，可以考虑降低每次签名的平均网络延迟，提高签名方案的整体效率。在文献[12]的跨域认证系统中，mIBS 方案主要用于信息服务实体 ISE 的签名认证。对 ISE 来说，短时间内多次签名是比较常见的，每一次签名就申请一次签名信令在实际应用中没有必要，既增加了 SEM 的负载也增加了方案的总体网络延迟。因此，在 $mIBS_G$ 方案的基础上，研究实现多次签名共享一个签名信令机制，可以降低每次签名的平均网络延迟，降低 SEM 的总体负载，提高签名的整体效率。第二，引入 SEM 进行身份实时撤销开销巨大，可以考虑采用自证书模式，借鉴 PKI 方案的思想，构建更加优化的跨域认证结构模型。

参考文献：

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Proc of the 4th Annual International Cryptology Conference. Berlin: Springer, 1985: 47-53.

[2] Boneh D, Franklin M. Identity-based encryption from the weil pairing [C]// Proc of the 21st Annual International Cryptology Conference. Berlin: Springer, 2001: 213-229.

[3] Boyen X, Martin L. Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems [EB/OL]. (2007) [2022-01-29]. http://www. ietf. org/rfc/rfc5091. txt

[4] 全国信息安全标准化技术委员会. GB/T 38635. 1—2020, 信息安全技术 SM9 标识密码算法第 1 部分: 总则 [S]. 北京: 国家标准化管理委员会, 2020.

[5] 全国信息安全标准化技术委员会. GB/T 38635. 2—2020, 信息安全技术 SM9 标识密码算法第 2 部分: 算法 [S]. 北京: 国家标准化管理委员会, 2020.

[6] Sattam S A, Kenneth G P. Certificateless public key cryptography [C]// Proc of the 9th International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2003: 452–473.

[7] 唐卫中, 张大伟, 佟晖. 基于 SM2 的无证书盲签名方案 [J]. 计算机应用研究, 2022, 39 (02): 552-556. (Tang Weizhong, Zhang Dawei, Tong hui. A certificateless blind signature scheme based on SM2 [J]. Application Research of Computers, 2022, 39 (02): 552-556.)

[8] 曾萍, 陈瑞利, 方勇. 基于自认证公钥的全分布式移动 Ad hoc 网络密钥管理方案 [J]. 计算机应用研究, 2008, 25 (06): 1779-1782. (Zeng Ping, Chen Ruili, Fang Yong. A fully distributed mobile Ad hoc network key management scheme based on self-authenticating public key [J]. Application Research of Computers, 2008, 25 (06): 1779-1782.)

[9] Zhang Qikun, Li Yongjiao, Zhang Quanxin, et. al. A self-certified cross-cluster asymmetric group key agreement for wireless sensor networks [J]. Chinese Journal of Electronics, 2019, 28 (02): 280-287.

[10] 罗长远, 霍士伟, 邢洪智. 普适环境中基于身份的跨域认证方案 [J]. 通信学报, 2011, 32 (09): 111-115+122. (Luo Changyuan, Huo Shiwei, Xing Hongzhi. Identity-based cross-domain authentication scheme in a universal environment [J]. Journal on Communications, 2011, 32 (09): 111-115+122.)

[11] 马晓婷, 马文平, 刘小雪. 基于区块链技术的跨域认证方案 [J]. 电子学报, 2018, 46 (11): 2571-2579. (Ma Xiaoting, Ma Wenping, Liu Xiaoxue. Cross-domain authentication scheme based on blockchain technology [J]. Acta Electronica Sinica, 2018, 46 (11): 2571-2579.)

[12] 魏松杰, 李莎莎, 王佳贺. 基于身份密码系统和区块链的跨域认证协议 [J]. 计算机学报, 2021, 44 (05): 908-920. (Wei Songjie, Li Shasha, Wang Jiahe. A cross-domain authentication protocol by identity-based cryptography on Consortium blockchain [J]. Chinese Journal of Computers, 2021, 44 (05): 908-920.)

[13] 黄穗, 李健, 范冰冰. IABC: 一种基于区块链和布谷鸟过滤器的跨域认证方法 [J]. 小型微型计算机系统, 2020, 41 (12): 2620-2625. (Huang sui, Li Jian, Fan Bingbing. IABC: a cross-domain authentication method based on blockchain and cuckoo filter [J]. Journal of Chinese Computer Systems, 2020, 41 (12): 2620-2625.)

[14] 魏欣, 王心妍, 于卓, 等. 基于联盟链的物联网跨域认证 [J]. 软件学报, 2021, 32 (08): 2613-2628. (Wei Xin, Wang Xinyan, Yu Zuo, *et al.* Cross domain authentic-ation for IoT based on permissioned blockchain [J]. Journal of Software, 2021, 32 (08): 2613-2628.)

[15] 张亚兵, 邢镔. 基于多层区块链的跨域认证方案 [J]. 计算机应用研究, 2021, 38 (06): 1637-1641. (Zhang Yabing, Xing Bin. Cross domain authentication scheme based on multilayer blockchain [J]. Application Research of Computers, 2021, 38 (06): 1637-1641.)

[16] Cha J C, Cheon J H. An identity-based signature from gap Diffie-Hellman groups [C]// Proc of the 6th International Workshop on Theory and Practice in Public Key Cryptography. Berlin: Springer, 2003: 18-30.

[17] Shacham H. New Paradigms in Signature Schemes [D]. CA: Stanford University, Department of Computer Science, 2005.

[18] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures [J]. Journal of Cryptology, 2000, 13 (3): 361-396.